Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) Circuitry for generating a random key, comprising:

a random number generator for generating a random number implemented in an integrated circuit;

an eFuse memory internal to the integrated circuit for receiving and permanently storing the random number, said eFuse memory being accessible only internally to the integrated circuit.

2. (original) The circuitry of claim 1 and further comprising circuitry for detecting undesirable random numbers.

3. (original) The circuitry of claim 2 wherein said detecting circuitry comprises circuitry for detecting a ratio of "1"s and "0"s in said random number and comparing the ratio to a threshold.

4. (currently amended) The circuitry of claim 1 and further comprising comparison circuitry for comparing [the] a threshold value ~~stored in said memory~~ to the random number, wherein the random number is operable to be regenerated if the threshold value is not passed.

5. (currently amended) A mobile computing device comprising:

processing circuitry implemented in an integrated circuit;

a random root key generator circuit implemented in said integrated circuit and coupled to said processing circuitry, comprising:

a random number generator for generating a random number for the root key;

a memory internal to the integrated circuit for receiving and permanently storing the random number, said memory being accessible only internally to the integrated circuit.

6. (original) The mobile computing device of claim 5 wherein said random key generator further comprises circuitry for detecting undesirable random numbers.

7. (original) The mobile computing device of claim 6 wherein said detecting circuitry comprises circuitry for detecting a ratio of "1"s and "0s in said random number and comparing the ratio to a threshold.

8. (currently amended) The mobile computing device of claim 6 wherein said random key generator circuit further comprises comparison circuitry for comparing [the] a threshold value ~~stored in said memory~~ to the random number, wherein the random number is operable to be regenerated if the threshold value is not passed.

9. (currently amended) A method of generating a random root key, comprising the steps of:

generating a random number for the root key in an integrated circuit;

permanently storing the random number in a memory on said integrated circuit, where said memory is accessible only internally to the integrated circuit.

10. (original) The method of claim 9 and further comprising the steps of identifying undesirable random numbers and regenerating a new random number in response thereto.

11. (new) The method of claim 9 wherein the step of storing comprises storing in an eFuse memory.

12. (new) Circuitry for generating a random key, comprising:

a random number generator for generating a root key random number implemented in an integrated circuit;

a root key memory internal to the integrated circuit for receiving and permanently storing the root key random number, said root key memory being accessible only internally to the integrated circuit; and

the root key random number is operable to seed a second random number to be a session key.

13. (new) The circuitry of claim 12 wherein the root key memory is an eFuse memory.

14. (new) The circuitry of claim 12 and further comprising circuitry for detecting undesirable random numbers.

15. (new) The circuitry of claim 14 wherein said detecting circuitry comprises circuitry for detecting a ratio of "1"s and "0"s in said random number and comparing the ratio to a threshold.

16. (new) The circuitry of claim 12 and further comprising comparison circuitry for comparing a threshold value to the random number, wherein the random number is operable to be regenerated if the threshold value is not passed.